# Document sobre Bioètica i Big Data de salut: explotació i comercialització de les dades dels usuaris de la sanitat pública

# Documento sobre Bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública

M.R. Llàcer, M. Casado i L. Buisan (coords.)

Organització de les Nacions Unides per a l'Educació, la Ciència i la Cultura

Càtedra UNESCO de Bioètica de la Universitat de Barcelona

Observatori de Bioètica i Dret

www.bioeticaidret.cat
www.bioeticayderecho.ub.edu
www.bioethicsandlaw.es

# Document sobre Bioètica i Big Data de salut: explotació i comercialització de les dades dels usuaris de la sanitat pública

# Documento sobre Bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública

M.R. Llàcer, M. Casado i L. Buisan (coords.)

Barcelona, gener de 2015

Organització de les Nacions Unides per a l'Educació, la Ciència i la Cultura

Càtedra UNESCO de Bioètica de la Universitat de Barcelona

Observatori de Bioètica i Dret

Universitat de Barcelona



Grup de Recerca Consolidat “Bioètica, Dret i Societat” de la Generalitat de Catalunya.

I. Llàcer, Maria Rosa. II. Casado, María. III. Buisan, Lidia.

1. Dades sanitàries. 2. Big Data. 3. Bioètica. 4. Privacitat. 5. Anonimització.

---

Avda. Diagonal, 684, Pav. 22, Facultat de Dret

08034 Barcelona

Tel./Fax: (+34) 93 403 45 46

www.bioeticayderecho.ub.edu

obd@ub.edu

# DOCUMENT SOBRE BIOÈTICA I BIG DATA DE SALUT: EXPLOTACIÓ I COMERCIALITZACIÓ DE LES DADES DELS USUARIS DE LA SANITAT PÚBLICA

# PRESENTACIÓ

El Grup d'Opinió de *l'Observatori de Bioètica i Dret,* de la Universitat de Barcelona, es va constituir el 1996 dins *l'Observatori de Bioètica i Dret,* que té, entre altres objectius, analitzar amb uns base científica i amb una metodologia interdisciplinària, les implicacions ètiques, socials i jurídiques de les noves tecnologies i els problemes biotecnològics i biomèdics, a fi d'intervenir en el diàleg entre la universitat i la societat mitjançant la transmissió del coneixement científic i tècnic, i aportant els arguments necessaris per a contribuir al debat social informat. Amb aquesta finalitat, el Grup d'Opinió ha elaborat ja vint-i-dos Documents[1] sobre temes d'actualitat i sobre els quals no hi ha una opinió unànime, ni en la societat ni en les diverses comunitats científiques implicades; això ha fet necessari identificar els problemes, contrastar els arguments i proposar recomanacions de consens.

En aquesta ocasió, el Grup fa públic el Document d'Opinió *Bioètica i Big Data de salut: explotació i comercialització de les dades dels usuaris de la sanitat pública,* a fi de cridar l'atenció sobre la necessitat de crear una cultura de la privacitat respecte de les dades personals, que han esdevingut elements o mecanismes de control en una societat informatitzada, per la qual cosa cal ser conscients de perquè i per a què aquestes dades han de ser protegides. Aquest Document analitza, des de la perspectiva bioètica, els problemes de l'explotació i la comercialització de dades dels usuaris de la sanitat pública. Prenent com a punt de partida el reconeixement del principi d'autonomia de les persones, el Document posa de manifest que la implementació de les tecnologies *big data* en l'àmbit sanitari, associada a una eventual comercialització d'aquestes dades, impacta directament en el nostre sistema sanitari i investigador –fonamentat en els principis d'igualtat i no discriminació– i afecta de ple a l'àmbit privat dels ciutadans.

El motiu immediat d'aquest Document han estat els problemes detectats en el projecte VISC+ (formalment anomenat *Més Valor a la Informació de Salut de Catalunya*) tant en relació a possibles vulneracions dels drets dels ciutadans com a la manca de transparència i de debat públic informat en una qüestió de tanta importància com és el tràfic de dades personals, reutilitzades amb finalitats diferents de l'atenció mèdica que puguin rebre directament els ciutadans. Els arguments que aquí oferim no solament fan referència a l'esmentat projecte sinó que tenen un abast major, perquè tenen a veure amb: a) la validesa de les tècniques d'anonimització en els *datasets*; b) la necessitat de redefinir el concepte de dades personals, tenint en compte la possibilitat actual de reidentificar les persones i c) l'impacte d'aquests dos aspectes en els mercats emergents de *big data, data marketplaces i digital marketing.*

[1] Tots els Documents del Grup d'Opinió de l'*Observatori de Bioètica i Dret* són accessibles en format PDF i en obert a: http://www.bioeticaidret.cat/documents (versió en català, espanyol i anglès).

Creiem que cal prendre mesures que garanteixin l'exercici dels drets i les decisions lliures i informades de totes les persones implicades. Pretenem obrir el debat sobre aquestes qüestions fent propostes que permetin afrontar el canvi de paradigma que impliquen aquestes noves tecnologies de la informació, car en una societat democràtica les decisions de l'Administració no han de ser imposades al ciutadà sense una informació prèvia, veraç i transparent sobre l'abast de les mateixes.

Aquest Document ha estat coordinat per les Dres. Maria Rosa Llàcer, María Casado i Lídia Buisan i ha estat elaborat pel Grup d'Opinió de *l'Observatori de Bioètica i Dret (*Grup de Recerca Consolidat *Bioètica, Dret i Societat*) amb la col·laboració del *Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT)*, de la Universitat de Barcelona. En la seva elaboració hi han participat, a més, les persones els noms i perfils professionals de les quals s'inclouen al final del document.

# CONSIDERACIONS GENERALS

## Els reptes del big data i l'anonimització

L'expressió *big data* és un terme que fa referència al tractament massiu de dades per mitjà d'algoritmes matemàtics a fi de generar correlacions entre elles, predir tendències i prendre decisions. Les tecnologies *big data* constitueixen un paradigma nou que, a més, implica canvis organitzatius importants tant en les empreses com en l'Administració. En l'actualitat, els objectius empresarials no són ja només la millora dels processos sinó la gestió de les dades. Estem assistint a una fase de transició cap a la *datificació* i la *monetització*, fet que comporta extreure un valor nou de les dades i rendibilitzar-les, tant en l'àmbit privat com en el públic o bé en una combinació de tots dos. Es tracta d'una tendència que s'insereix en el marc d'una indústria creixent basada en el coneixement adquirit mitjançant la reutilització de les dades i l'explotació d'aquestes, qüestió que cal tenir en compte a fi de contextualitzar el debat i entendre millor aquest canvi de model. Això no obstant, l'aposta per la innovació no ha de fer oblidar els aspectes ètics i els drets fonamentals de les persones, ni la protecció dels ciutadans en el context d'aquests nous avenços de les tecnologies. Es tracta de plantejar l'anàlisi d'aquesta situació amb la finalitat de proposar un nivell de protecció fort que suposi, per això mateix, un nivell més avançat d'innovació en aquest àmbit.

És molt important assenyalar que, fins ara, la premissa de *l'anonimització* de les dades ha estat la garantia que permetia respectar les regulacions de protecció de dades personals existents, en el benentès que en ser anonimitzada la dada personal passa a ser simplement una dada, perdent així la protecció de la normativa de protecció de dades personals, normativa que pretén ser rigorosa, tant a la Unió Europea com a l'Estat espanyol, però que amb els avenços de les tecnologies informàtiques després de gairebé vint anys ha esdevingut en bona part obsoleta. El problema rau en que, actualment, aquesta anonimització és palesament il·lusòria, perquè mitjançant tècniques d'enginyeria informàtica hom pot tornar a connectar les dades amb la persona font.[2] Tant la desanonimització de les dades com la reidentificació de persones són

[2] Art. 29 Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse (1021/00/EN WP207); Art.29 Working Party Opinion 05/2014, on Anonymisation Techniques (0829/14/EN WP216). Vegi's: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

NARAYANAN, Arvin; FELTEN, Edward W. "No silver bullet: De-identification still doesn't work", 2014. Vegi's: http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf

NARAYANAN, Arvin; SHMATIKOV, Vitaly. "Robust de-anonymization of large sparse datasets". *Security and Privacy*. IEEE Symposium on IEEE, 2008, pp. 111-125.

DE MONTJOYE, Yves-Alexandre, *et al.* "Unique in the Crowd: The privacy bounds of human mobility". *Scientific reports*, 2013, vol. 3.

OHM, Paul: "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". *UCLA L. Rev.*

possibles si es disposa de la competència tècnica i dels mitjans necessaris per a fer-ho, per la qual cosa el debat es trasllada a un territori més tècnic i objectiu que proporciona informació i arguments que afecten directament a la cada vegada més estesa indústria de venda de dades. N'hi ha prou en saber que la reidentificació es pot fer tenint en compte el valor especial que poden adquirir determinades dades que fins ara s'ha considerat com no personals; per exemple, avui dia és prou evident que amb el codi postal, la data de naixement i el sexe ja és possible reidentificar la major part de les persones d'un *dataset*. De manera semblant a com les nostres empremtes digitals ens identifiquen de manera unívoca, el mateix passa amb determinades tipologies de dades. La polèmica que hi ha darrere no és gens banal: què és una dada personal i com en podem garantir la protecció?[3] Com es pot evitar que a partir d'un conjunt de dades no personals es pugui identificar una persona?

Volem remarcar especialment aquest punt perquè el negoci de "posar en valor" les dades depèn precisament del concepte d'anonimització esmentat, ja que seria precisament aquest el que permetria complir amb les regulacions de protecció de dades personals. El debat sobre l'anonimització, tot i que ja té una certa història, no ha fet més que començar i és ben lluny d'estar acabat. En la nostra opinió, aquesta discussió és crucial en el segle XXI i no està tenint, ni de bon tros, la presència que li escauria en els diferents fòrums que hi tenen a veure (legals, ètics, tècnics, empresarials, governamentals) i en els quals caldria endegar el debat oportú perquè sigui compresa, primer, i resolta o si més no gestionada, després.

Com s'ha dit, actualment les evidències tècniques ja ens mostren que és possible reidentificar persones concretes a partir de les dades d'un conjunt de dades (*dataset)* al qual s'hagin aplicat prèviament tècniques d'anonimització (o de desidentificació). Una persona, o bé una empresa, poden aconseguir la reidentificació esmentada si hi tenen interès (per motius econòmics, empresarials, delictius...), i tenen també els coneixements i els mitjans tecnològics per a fer-ho (per exemple, si disposen de les dades sanitàries d'un hospital –encara que no continguin dades personals– i d'accés a les dades personals d'un altre *dataset*, com ara un cens). Resulta evident que, en el cas de les dades de salut, no és difícil trobar un suposat "adversari" amb la motivació i els recursos per a fer-ho, i és escaient, per tant, qüestionar la validesa de les iniciatives de bescanvi de dades sensibles fonamentades en tècniques d'anonimització. En l'àmbit jurídic, l'incert recurs a "l'anonimització", entesa com una solució definitiva però inevitablement en crisi, es recolza en la normativa actual de protecció de dades, que prové d'una Directiva europea de l'any 1995 –per tant, molt anterior al fenomen del *big data*– i que es recull en la Llei 37/2007, de 16 de novembre, sobre la reutilització de la informació del sector públic. Però si el concepte mateix d'anonimització esdevé incert, cal trobar un fonament que legitimi l'anàlisi de dades

2009-2010, p. 731.

[3] SCHWARTZ, Paul M.; SOLOVE. D. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *N.Y.U. L. Rev*. 1814 2011.

personals de salut a gran escala. Si no és així, aleshores s'està obrint la porta a usos no desitjats d'aquestes dades, car en haver donat anteriorment el titular de les dades el seu consentiment per a determinades accions en l'àmbit sanitari i de recerca, en realitat en perd el control i queda desprotegit sense que sàpiga –perquè té una concepció equivocada de la protecció de dades i del secret professional– que les seves dades poden haver sigut utilitzades o cedides per a altres fins que no són ni desitjats ni efectivament consentits.

Aquest Document no pretén rebutjar, sense més, aquest nou model de negoci que centra l'atenció del mercat i en el qual, a més, ja estem immersos, sinó que vol alertar, tant als ciutadans com als poders públics que regulen i controlen l'activitat en l'àmbit sanitari i de recerca, dels riscos que comporta. En el nostre entorn no està prou consolidada una consciència social de la importància de protegir les dades en relació amb el dret fonamental a la intimitat i a la no discriminació. No tenim una cultura de la privacitat que ens permeti comprendre de quina manera ens pot afectar que una empresa acumuli i faci rendible la nostra informació, i que disposi d'un instrument de poder en base al qual pugui prendre decisions que ens afectin.[4] N'és un exemple el fet que l'anàlisi massiva de dades es pot fer servir per a descobrir efectes secundaris de medicaments, però també per a generar perfils de risc –i que els propis afectats poden no conèixer– que es podrien utilitzar per a "justificar" la denegació d'una assegurança.

Es fa evident, en conseqüència, la urgència d'un debat que posi de relleu la vulnerabilitat de les persones davant el risc de discriminació generat per perfils i patrons de conducta generats amb finalitats que la persona afectada no pot controlar, i també sobre l'adaptació de les lleis als reptes ètics i socials que les *big data* plantegen. Aquest és, precisament, el nucli del conflicte que cal obrir al debat públic amb implicació de la ciutadania a fi de crear una cultura de la privacitat que vagi d'acord amb l'actualitat i amb les noves realitats.

## Sobre el Projecte VISC+

Un exemple de reutilització de dades que, des del nostre punt de vista, resulta molt qüestionable és el projecte VISC+, impulsat per l'Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS), que té com a objectiu –segons esmenten els seus promotors– posar la informació sanitària a disposició dels ciutadans, les empreses i la recerca per a millorar els serveis de salut i la investigació, i per a "posar en valor" el coneixement.

L'esmentat projecte es nodreix de les diferents bases de dades que ja existeixen en el sistema sanitari: el Sistema d'Informació per al Desenvolupament de la Investigació en Atenció Primària (SIDIAB) i, de manera especial, la Història Clínica Compartida a Catalunya (HC3), que recull les

[4] COHEN, Julie: "What Privacy is for" *Harv. L. Rev.* 1904, 2012-2013.

dades assistencials i de consum farmacèutic, juntament amb altres informacions rellevants com són la identificació i la situació sociosanitària de cada ciutadà atès per la sanitat pública; a més, la HC3 conté informació de les proves analítiques i diagnòstiques que inclouen paràmetres metabòlics i bioquímics, així com dades de diagnòstic genètic que identifiquen les persones portadores de malalties genètiques hereditàries o bé que mostren riscos i susceptibilitats de patir malalties més complexes. Aquestes bases de dades fa que existeixin "fitxers d'usuaris" dels quals n'és responsable el Departament de Salut de la Generalitat de Catalunya. Tot i que els macro fitxers de dades estan protegits per la normativa ja existent –en especial per la Llei Orgànica de Protecció de Dades (LOPD) i el Reglament que la desenvolupa– aquesta regulació ha esdevingut del tot inadequada en el marc de la nova realitat dels *big data*, com s'ha esmentat abans, i no garanteix de cap manera que no es produeixin usos indeguts i discriminatoris.[5]

La HC3 té els objectius explícits següents: a) millorar l'atenció de la salut dels ciutadans mitjançant una eina que faciliti la feina dels professionals sanitaris respecte als malalts als quals han d'atendre; b) propiciar un nou model assistencial en permetre l'accés i la consulta de forma immediata, segura i confidencial, de la informació rellevant disponible sobre els usuaris. Com és obvi, les dades que conté la HC3 són extremadament sensibles, la recollida i el tractament de les quals es justifica en la seva eficàcia per a proporcionar una assistència de qualitat, no sols en el centre que habitualment atén l'usuari sinó en tota la xarxa assistencial pública de Catalunya[6], perquè la HC3 permet l'accés de manera organitzada, i atenent a criteris de seguretat i confidencialitat, a les històries clíniques de la xarxa assistencial. Aquesta eina ha d'oferir beneficis tant a la ciutadania, com als professionals sanitaris, com al propi sistema de salut. Per aquesta raó, el ciutadà té dret a saber qui pot accedir a les seves dades personals i amb quina finalitat; i també té dret a exigir responsabilitats si creu que se n'està fent un ús indegut o distint d'aquell al qual en el seu moment va consentir. Quan es va dur a la pràctica la HC3, ni es va informar suficientment els ciutadans d'aquesta recollida massiva de dades amb finalitat assistencial, ni es va indicar en cap moment que aquestes mateixes dades podrien ser reutilitzades amb altres finalitats, fins i tot comercials. De cap manera es pot considerar que la cessió de les dades per a finalitats no assistencials sigui el "preu" de la gratuïtat de l'assistència sanitària, ja que si s'exigís algun tipus de contraprestació l'assistència deixaria de ser gratuïta.

La informació que conté la HC3, tot i ser recollida i estructurada pels professionals assistencials, fa referència a les dades de salut del malalt i, per tant, aquestes li pertanyen, per la qual cosa les entitats assistencials reben peticions relacionades amb l'exercici dels drets que la

[5] Com el Grup d'Opinió ja va advertir en el *Document sobre proves genètiques de filiació*, Barcelona: Signo, 2006. Disponible en format PDF a: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/07899.pdf

[6] Existeix un projecte d'un abast territorial major, desenvolupat en 12 països de la Unió Europea, en el marc de www.epSOS.eu i del que formen part Alemanya, Àustria, Txèquia, Dinamarca, Eslovàquia, Espanya, França, Grècia, Holanda, Itàlia, Regne Unit i Suïssa. De l'Estat espanyol hi participen tres CCAA: Andalusia, Castilla la Mancha i Catalunya, dins del PLAN AVANZA per a la modernització dels serveis de les Administracions públiques.

normativa sobre protecció de dades vigent reconeix a la ciutadania: drets d'accés, de rectificació, de cancel·lació i d'oposició (els anomenats drets ARCO). La finalitat d'aquest conjunt de drets és impedir un tractament il·lícit i lesiu per a la dignitat i el dret de l'afectat (*habeas data*), alhora que per a garantir l'exercici del dret més general a la intimitat. Els usos de les dades recollides en la HC3 s'han de limitar a l'assistència (juntament amb les finalitats científiques –en epidemiologia, investigació i docència, o bé dirigides a la millora dels serveis públics– que la normativa actual ja autoritza) i és absolutament necessari establir garanties reals que evitin el tràfic de dades i qualsevol ús indegut per part d'empreses de l'àmbit de la salut (assegurances mèdiques, corporacions farmacèutiques, entitats financeres, i altres). Per això, el projecte VISC +, tal com en aquests moments està previst que es dugui a terme, genera dubtes importants, tant de caràcter bioètic com estrictament jurídics, que convé analitzar amb detall i debatre, a fi de prevenir-ne possibles usos discriminatoris.

## Problemes rellevants del projecte VISC+

### 1.- Denominació equívoca del projecte

La mateixa denominació del projecte és equívoca i no s'adequa al principi general de lleialtat en la recollida i tractament de dades, perquè indueix a pensar que el projecte ajuda a millorar les condicions de vida i la salut dels ciutadans. Els usuaris a qui es demani el consentiment perquè les seves dades personals de salut siguin tractades en el marc d'un projecte anomenat VISC+ poden pensar, erròniament, que col·laboren en un programa que l'única cosa que pot aportar-los són beneficis. Això pot ser fàcilment relacionat amb una pràctica deslleial, entesa com una conducta contrària a la bona fe objectiva que distorsiona la capacitat d'escollir amb ple coneixement de causa i que indueix a facilitar unes dades que altrament no s'haurien proporcionat. La lleialtat és un valor fonamental en el marc de la LOPD, ja que la recollida i el tractament de dades per mitjans fraudulents o deslleials està prohibida expressament i afecta de manera directa el principi de qualitat de les dades.

### 2.- Limitació de les finalitats en el tractament de les dades

Com bé es diu en l'informe elaborat pel *Grup europeu d'ètica de les ciències i de les noves tecnologies* (GEE), de la Comissió Europea, en la recollida i el tractament de dades de caràcter personal les entitats públiques i les privades han de fonamentar la seva activitat en el principi de "limitació de la finalitat"[7]; és a dir, que aquest tipus de dades no haurien de ser recollides ni tractades per a qualsevol ús, sinó només amb objectius específics i legítims. Cal, a més, que les dades no estiguin per defecte a disposició de "qui les vulgui utilitzar" i que els ciutadans tinguin mecanismes

[7] EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES: Ethics of Security and Surveillance Technologies. Opinion n. 28, 20 de maig de 2014. Vegi's: http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf

efectius per a controlar i modificar les informacions que els concerneixin i que estiguin dipositades en les esmentades entitats. Insisteix també l'informe en que la possible cessió de dades amb finalitats comercials ha de fer-se només amb el consentiment explícit de les persones afectades, i que les entitats privades han d'indicar el tipus de dades que preveuen tractar i amb quin objectiu, durant quant de temps i si tenen intenció de relacionar o connectar aquestes dades amb altres procedents de diferents fonts.

Resulta especialment important, en el marc del projecte que aquí s'analitza, la gradualitat de la protecció de les dades en funció de la finalitat de l'ús, distingint acuradament les finalitats sanitària, epidemiològica i d'investigació i docència –que ja estan emparades per la legislació– de les finalitats privades, a les quals cal exigir el nivell de protecció més elevat. Ara bé, el projecte VISC+ equipara tractaments que tenen finalitats totalment diferents i aquesta confusió afecta la legitimació per tractar dades sanitàries personals, que són dades especialment sensibles i que, en conseqüència, estan sotmeses a una protecció especial.

Com ja s'ha dit, la legislació empara l'ús de dades dels usuaris de salut per a dur a terme l'assistència sanitària i per a la recerca i la millora dels serveis públics. Però si es vol anar més enllà i facilitar la utilització d'aquestes dades amb finalitats ni previstes ni autoritzades –com són els interessos comercials d'empreses privades els productes de les quals depenen de la recerca, a més d'altres factors– cal un debat social previ sobre la concurrència dels interessos públics i privats en l'àmbit de la recerca a fi definir els límits ètics i el nivell de protecció de què disposarà el ciutadà quan empreses amb interessos privats facin el tractament de dades de salut. L'*empowerment* del ciutadà es basteix amb informació adequada, clara i veraç sobre l'ús de les seves dades, a més de reconèixer-li la facultat de controlar el tractament de les mateixes, ja sigui consentint-hi o bé oposant-s'hi.

## 3.- Habilitació legal *vs* consentiment

Comptar amb legitimació suficient és el requisit bàsic per a permetre l'accés de terceres persones a informacions o dades que pertanyen a l'àmbit personal dels afectats. Cal diferenciar entre la legitimació legal i la voluntària, basada aquesta segona en el consentiment lliurement atorgat. La primera fa referència a finalitats relacionades amb l'atenció sanitària, la qualitat i gestió del servei i a finalitats científiques (epidemiològiques, de recerca i docència). Aquesta legitimació, ja reconeguda legalment, es justifica en l'interès públic, respectant sempre escrupolosament la confidencialitat de les dades així recollides i obligant a motivar la sol·licitud d'ús de les mateixes. Pensem que el projecte VISC+, en haver estat aprovat per un mer "Acord de Govern", no té l'habilitació legal suficient per a la reutilització de dades sanitàries, perquè la legislació sanitària només legitima per a tractar dades d'usuaris amb finalitats directament assistencials, de recerca o bé administratives. El segon tipus de legitimació, la voluntària, prové sempre del consentiment explícit del pacient. Aquest és el cas del tractament de dades amb finalitats estrictament privades, és a dir, sense interès públic evident i dirigides al desenvolupament de les indústries sanitàries,

farmacèutiques i de biotecnologia, o per a la promoció i comercialització dels productes que generin. Menció a part mereixen les dades genètiques a causa de la complexitat que suposa la titularitat de les mateixes quan es compartida per un nucli familiar.

Tenint en compte l'existència del binomi públic-privat en el sistema sanitari i de recerca, el problema cal centrar-lo en com convé articular la legitimació abans esmentada a fi de poder emprar la informació de salut i reutilitzar-la. Segons el nostre parer, cal que això quedi establert en una llei, tenint en compte, a més, l'enorme asimetria existent –d'informació, però també de poder– entre el ciutadà, que pateix una malaltia i que el que vol és curar-se, i el professional que li demana el consentiment, tant per a l'assistència mèdica més escaient en el seu cas com per al tractament de les dades personals de salut en general. Però ha d'estar clar que es tracta de dos consentiments diferents, i que la prestació sanitària pública no es pot condicionar al consentiment per a tractar dades amb altres finalitats, ni pot justificar la sol·licitud de dades addicionals. La conclusió que cal extreure del que s'acaba de dir és que l'obtenció del consentiment s'ha de sotmetre a pautes rigorosíssimes a fi de compensar la situació de desequilibri en què es troba l'usuari dels serveis sanitaris públics, i més en un moment en què sol estar especialment preocupat per la seva salut, la qual cosa li pot generar una situació de vulnerabilitat que el dugui a pensar *a priori* que totes les dades que se li demanen són imprescindibles per al seu tractament i per a rebre l'assistència que necessita i que és la raó per la qual ha acudit al sistema sanitari.

## 4.- Valor i risc

És en aquest context que el projecte VISC+ es presenta amb la finalitat de "posar en valor" l'enorme quantitat de dades de què disposa el Departament de Salut, reutilitzant aquestes dades per a finalitats no previstes inicialment i que, per tant, l'usuari no coneix. L'expressió "posar en valor" té interpretacions diferents: d'una banda, es tractaria de posar a disposició de centres de recerca, centres d'estudis epidemiològics i de salut pública, i centres de docència que així ho sol·licitin, dades de salut dels ciutadans amb l'objectiu de contribuir al progrés del coneixement, en els àmbits específics esmentats, i també, en darrer terme, a la millora de l'atenció sanitària, i la prevenció, qüestions perfectament legítimes i que, insistim, la legislació actual ja permet. Però, d'altra banda, també se'n fa una interpretació molt més laxa pel fet de posar aquestes *big data* sanitàries a disposició d'empreses que difícilment entrarien en els àmbits que s'acaben d'esmentar. Si tenim en compte el principi econòmic ben conegut segons el qual *big data is big business,* l'escenari més probable seria el d'una pura i simple venda de les dades de salut dels ciutadans en benefici de l'empresa que estigui interessada en fer rendible aquesta informació i que disposi dels mitjans per a fer-ho. Convé remarcar que el problema no és la tecnologia, sinó el sentit i la direcció que li doni qui la utilitzi i qui la financi. El marc que proposa el projecte VISC+ permetria a les empreses interessades extreure un valor merament comercial de les dades.

Els riscos potencials a què fa referència aquest Document no són ni hipotètics ni remots: n'hi ha prou amb analitzar la possibilitat de construir perfils de conducta en base a dades

anònimes que en qualsevol moment es poden utilitzar per a prendre decisions automatitzades que afectin persones. N'hi ha prou de fer una passejada breu per internet per veure una bona quantitat d'empreses dedicades a la compravenda de dades i com les que ja les posseeixen –perquè són dades que ja s'han generat per a altres fins i serveis– creen, al seu torn, altres empreses i línies de negoci dedicades a la reutilització d'aquestes dades, aconseguint perfils molt precisos mitjançant encreuaments successius d'informació i altres processos d' enriquiment de dades.

## 5.- Control de les dades

Precisament per a evitar la pèrdua de control sobre les dades i per la possibilitat d' abús, té sentit establir funcions de *Data Governance* (és a dir, el control del tractament i la gestió de les dades) que han de correspondre a les entitats públiques, garants del respecte escrupolós dels drets fonamentals dels ciutadans, amb independència de com se subministrin els serveis professionals per part de les empreses adjudicatàries. Aquestes funcions de governança han d'incloure aspectes com: la seguretat i qualitat de les dades, la privacitat, els processos d'anonimització, la traçabilitat, les polítiques de permanència de les dades i l'enriquiment de dades, posant limitacions a les fonts o bases de dades amb què es poden relacionar o connectar. Aquesta preferència per les garanties que ofereix l'àmbit públic prové de les obligacions específiques de transparència i de rendició de comptes que té l'Administració, encara que el criteri de responsabilitat compartida exigiria aquesta mateixa transparència i rendició de comptes també al sector privat. La *Declaració Universal sobre Bioètica i Drets Humans* de la UNESCO (2005) estableix, en l'art. 14, el principi innovador de responsabilitat social en salut, principi que escau perfectament en el context que aquí s'analitza i que al mateix temps alerta sobre la necessitat d'evitar els conflictes d'interessos en un àmbit tan delicat com aquest.

El projecte VISC+ parla de governança, però merament de caràcter intern; en aquest Document, en canvi, es proposa un control extern i representatiu de la societat. Cal remarcar que l'informe de l'Autoritat Catalana de Protecció de Dades (ACPD) ja assenyala que el projecte VISC+ mereix un règim específic de seguretat encara més estricte. Segons aquest informe, el departament de Salut és a efectes legals el "responsable" del tractament de les dades, mentre que "l'entitat" (l'Agència de Qualitat i Avaluació Sanitàries de Catalunya -AQuAS) és "l'encarregada" del tractament de les dades. També la mecànica prevista en el projecte VISC+ per a l'explotació de les dades és motiu de preocupació, perquè l'empresa adjudicatària rebria les dades suposadament anonimitzades a canvi d'un preu o taxa, tot i que també s'hi diu que l'adjudicatari participaria en el procés de verificació de l'anonimització i en la materialització d'un "codi anònim de la persona" abans de transferir les dades als usuaris finals. No es diu enlloc si seria aquesta mateixa empresa adjudicatària qui es responsabilitzaria de "definir, construir i posar en marxa un catàleg de serveis útil, eficient, competitiu i innovador, i contrastar les necessitats del mercat i els clients finals del projecte, així com de definir un pla de difusió i de comercialització, canalitzant de manera adequada la demanda del mercat nacional i internacional".

En el model VISC+ no està gens clar si serien les empreses adjudicatàries qui decidirien a qui traspassen les dades de salut, presumptament a canvi de contrapartides econòmiques que tampoc no es precisen enlloc ni s'esmenta com retornarien als ciutadans. Per exemple, se cedirien bases de dades de malalts de l'hepatitis C per a desenvolupar fàrmacs que després es voldrien vendre a 70.000 euros cada tractament? Precisament aquest punt seria clau, perquè en dependria de fins quin punt els clients o usuaris finals del projecte estarien disposats a contribuir-hi en funció de les expectatives de negoci que prevegin.

## 6.- Avaluació de l'impacte

El projecte VISC+ no inclou cap avaluació de l'impacte que, un cop engegat, pugui tenir sobre el dret a la intimitat dels usuaris, qüestió cabdal tenint en compte que estem parlant de dades tan sensibles com les de salut, en la línia del que proposa el projecte de Reglament europeu de protecció de dades. Aquesta valoració de l'impacte –també des de les perspectives ètica i social– s'ha de considerar un requisit de qualsevol llei que empari projectes com el VISC+. Ni tampoc s'especifica enlloc si els usuaris han de donar prèviament el seu consentiment per al transvasament de dades que suposa el projecte, o si s'entén que aquest consentiment no seria necessari pel fet de la interpretació laxa del concepte de recerca a què s'ha fet referència més amunt i que no diferencia entre l'interès públic i l'interès privat.

Una darrera qüestió extremadament important és que en cap moment s'explica clarament de quina manera el benefici econòmic que s'obtingués del projecte repercutiria favorablement als ciutadans i al sistema sanitari públic. Amb dades tan valuoses, i quan hi ha expectatives de beneficis i de negoci, sembla raonable que els ciutadans en rebin contrapartides clares. Si bé hom pot considerar que el lucre és un objectiu lícit, no és cert que sigui el bé primordial al qual tots els altres valors i drets hagin de sotmetre's. El Conveni sobre Drets Humans i Biomedicina, del Consell d'Europa, vigent des de l'any 2000, estableix –en l'article 2– que els interessos de la ciència o de la societat mai no han de prevaldre sobre els de les persones, i en aquesta premissa es basa tot el sistema de ciència i tecnologia, especialment el sistema sanitari i de recerca.

## 7.- L'experiència del *National Health Service*

A banda del que ja s'ha dit, val la pena remarcar que les experiències en la línia del projecte VISC+ que s'han dut a terme en països del nostre entorn han generat conflictes molt significatius que porten a extremar les mesures de prudència abans d'endegar projectes d'aquest tipus. En efecte, la suposada anonimització de dades de salut i d'atenció sanitària recol·lectades –des de 2005 fins a 2013– pel *NHS Information Centre* (NHS-IC) anglès no ha impedit que diferents empreses hagin pogut identificar les persones a qui feien referència aquestes dades, causant-los diferents perjudicis, per exemple l'increment del preu de les primes de risc de les assegurances. La conseqüència ha estat una moratòria, a fi de reorganitzar el procediment de cessió de les dades de manera que sigui més transparent, que es garanteixi de forma més eficaç el dret a la intimitat i a la confidencialitat dels ciutadans. En l'actualitat, tot el procediment de tractament i cessió de les

dades està sotmès en tot moment a auditoria i control públic; a més, s'ha creat el *Care Data Advisory Group*, grup consultor la missió del qual és enfortir la protecció dels drets dels ciutadans en l'àmbit sanitari, i el *National Data Guardian*, a fi de vetllar per la seguretat de les dades de salut.

## RECOMANACIONS

1. *Generar i potenciar una cultura ciutadana de la privacitat en matèria de dades personals*. Acumular informació sobre una persona equival a adquirir poder de decisió sobre ella; en conseqüència, els mitjans per a controlar qui tracta les nostres dades, com les recapta i amb quina finalitat les utilitza es converteixen en eines tant de la llibertat personal com de la col·lectiva.

2. *Informar i formar la ciutadania sobre l'abast real del fet que els processos d'anonimització de les dades ja no garanteixen per ells mateixos la irreversibilitat*. Actualment són possibles la desanonimització, la reidentificació o la revelació de dades personals de conjunts d'usuaris o d'usuaris individuals, car les eines informàtiques emprades poden servir tant per a aquesta finalitat com per a la contrària.

3. *Alertar sobre la necessitat de redefinir el concepte mateix de "dades personals" en què es fonamenta la legislació actual.* És important tenir present que el problema no és únicament la transformació de les dades que es consideren personals en un conjunt de dades, perquè fins i tot eliminant-ne aquestes dades personals hom pot reidentificar persones concretes.

4. *Aplicar escrupolosament el principi que exigeix que les dades que es recol·lectin siguin adequades a la finalitat que motiva la seva recollida, exigint que se sol·liciti i que s'obtingui el consentiment explícit dels usuaris per a la utilització de les seves dades de salut amb finalitats distintes d'aquelles per a les quals es varen obtenir en el seu moment, implementant mecanismes eficaços per a atorgar o, si és el cas, per a denegar el dit consentiment.* En el cas de les dades genètiques, el consentiment ha de ser especialment exigent a causa de la possible afectació d'altres membres del nucli familiar.

5. *Potenciar un procés d'informació i de debat entre la ciutadania –basat en una valoració honesta dels riscos i beneficis, dels avantatges i perjudicis– abans de posar en marxa un projecte com el VISC+,* dirigit a l'explotació de dades de salut que pertanyen als ciutadans, encara que estiguin en mans de l'Administració, a fi que aquests puguin expressar el seu parer sobre la conveniència de dur a la pràctica o no un projecte com aquest.

6. *Establir mecanismes de control i concretar les funcions de Data Governance, que són responsabilitat dels organismes públics*. Els processos d'anonimització de les dades s'han de dur a terme dins del perímetre intern de l'Administració, en raó de les garanties que ofereixen les obligacions de transparència i de rendició de comptes que té l'Administració, tenint present, però, que la responsabilitat compartida exigeix també transparència i rendició de comptes al sector privat, en especial en el cas de xarxes mixtes público-privades.
   *Controlar de manera específica la seguretat en el tractament de les dades sanitàries a fi de garantir en tot moment el seu ús correcte i evitar-ne la comercialització que no compti amb el consentiment explícit dels usuaris i que no prevegi de forma clara com el benefici que se'n pugui obtenir revertirà*

*als ciutadans.*

A tal fi, hi ha d'haver un òrgan de governança extern, independent dels agents implicats i representatiu de la societat catalana. Les seves funcions han de ser supervisar la gestió dels fitxers al llarg de totes les etapes del procés, verificar-ne la traçabilitat, detectar possibles conflictes d'interessos i males pràctiques, així com identificar possibles infraccions i responsabilitats, i haurà d'informar públicament de la seva actuació i resultats. D'aquesta manera, el ciutadà podria dirigir-se a aquest òrgan per a saber qui disposa de les seves dades personals i amb quina finalitat.

Per a dur a terme aquestes funcions, l'esmentat òrgan ha de promoure i aplicar un *Codi Ètic per a la Reutilització de Dades de Salut*.

7. *Enfortir la formació en deontologia i ètica professional dels implicats en la custòdia de les dades*, insistint en que qualsevol persona que tingui accés o tracti les dades té el deure de protegir i promoure els drets i llibertats fonamentals dels ciutadans afectats. El dret a la intimitat, la confidencialitat i la no discriminació són pilars bàsics del sistema de salut i de recerca.

8. *Recordar que els diferents Comitès d'Ètica han de contribuir al desenvolupament de la cultura de respecte de la intimitat i la confidencialitat de les dades personals, perquè en el àmbit d'actuació que els és propi són la primera línia de defensa d'aquests drets.* Els membres d'aquests Comitès han de tenir formació específica en els aspectes ètics, tècnics, jurídics i socials de les noves tecnologies a fi de poder col·laborar en la presa de decisions ponderades i proporcionals –tenint sempre present que les dades sanitàries són dades sensibles que requereixen una protecció especial– i posant atenció, a més, a no actuar de manera que puguin esdevenir mers mecanismes de cobertura d'interessos aliens.

# NORMATIVA DE REFERÈNCIA

## Internacional

- Consell d'Europa: Conveni per a la protecció dels Drets Humans i la dignitat del ser humà pel que fa a les aplicacions de la biologia i la medicina (Conveni sobre Drets Humans i biomedicina), fet a Oviedo el 4 d'abril de 1997.
- UNESCO: Declaració Universal sobre Bioètica i Drets Humans, de 19 de octubre de 2005.

## Europea

- Carta dels Drets Fonamentals de la Unió Europea (DOUE núm. 83, de 30 de març de 2010).
- Directiva 1995/46/CE, de 24 d'octubre, del Parlament Europeu i del Consell, relativa a la protecció de les persones físiques relativa al tractament de les dades personals i a la lliure circulació d'aquestes dades.
- Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques (Directiva sobre la privacitat i les comunicacions electròniques).

## Espanyola

### Sistema sanitari

- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.
- Ley 33/2011, de 4 de octubre, General de Salud Pública.
- Llei 21/2000 (del Parlament de Catalunya), de 29 de desembre, sobre els drets d' informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

- Llei 16/2010 (del Parlament de Catalunya), de 3 de juny, de modificació de la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

### Sistema d'investigació

- Real Decreto 223/2004, de 6 de febrero, por el que se regulan los ensayos clínicos con medicamentos.
- Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.
- Ley 14/2007, de 3 de julio, de Investigación Biomédica.
- Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

### Protecció de dades de caràcter personal

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

### Reutilització de la informació del sector públic

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, sobre reutilización de la información del sector público.

# DOCUMENTO SOBRE BIOÉTICA Y BIG DATA DE SALUD: EXPLOTACIÓN Y COMERCIALIZACIÓN DE LOS DATOS DE LOS USUARIOS DE LA SANIDAD PÚBLICA

# PRESENTACIÓN

El *Grupo de Opinión del Observatori de Bioètica i Dret de la Universitat de Barcelona* surgió en 1996 en el seno del *Observatori de Bioètica i Dret*. Éste tiene entre sus objetivos analizar científica e interdisciplinarmente las implicaciones éticas, sociales y jurídicas de las nuevas tecnologías y los problemas biotecnológicos y biomédicos e incidir en el dialogo entre la universidad y la sociedad, mediante la transmisión del conocimiento científico-técnico y los argumentos necesarios para participar en un debate social verdaderamente informado. Con este fin, el *Grupo de Opinión* ha elaborado ya veintidós Documentos[8] sobre temas de actualidad sobre los que no existe una opinión unánime, ni en la sociedad ni en las diversas comunidades científicas implicadas; ello ha requerido identificar los problemas, contrastar los argumentos y proponer recomendaciones de consenso.

Ahora, el *Grupo* presenta el *Documento de Opinión* sobre *"Bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública",* que pretende alertar sobre la necesidad de crear una cultura de la privacidad en materia de datos personales ya que estos se han convertido en elementos o dispositivos de control en una sociedad informatizada, y es preciso ser conscientes de por qué y para qué deben protegerse. Analizamos, desde una perspectiva bioética, los problemas de la explotación y comercialización de los datos de los usuarios de la sanidad pública. Partiendo del reconocimiento del principio de autonomía de las personas, el Documento se encamina a poner de manifiesto que la implementación de las tecnologías Big Data en salud, asociada a una eventual comercialización de dichos datos, produce un impacto en nuestro sistema sanitario e investigador –asentado en los principios de igualdad y no discriminación– y afecta directamente a la esfera privada de los ciudadanos.

El detonante inmediato de Documento han sido los problemas detectados en el proyecto VISC+ –*Más Valor a la Información de Salud en Cataluña*– y que son de dos tipos: 1) las posibles vulneraciones de los derechos de los ciudadanos y 2) la falta de transparencia y debate público informado en una cuestión en la que subyace el tráfico de datos personales reutilizados con fines distintos al tratamiento médico directamente recibido por el paciente. Así, planteamos argumentos que son relativos al mencionado proyecto, pero que tienen un alcance mayor: a) la validez de las técnicas de anonimización sobre *datasets,* b) la necesidad de redefinir el concepto de datos personales, dada la actual capacidad de re-identificación de personas y c) el impacto de las dos cuestiones anteriores en los mercados emergentes de *big data, data marketplaces y digital marketing*.

[8] Todos los Documentos del Grupo de Opinión del *Observatori de Bioètica i Dret* son accesibles en formato PDF y en abierto en: http://www.bioeticayderecho.ub.edu/documentos (versión en catalán, español e inglés).

Consideramos que es preciso tomar medidas que permitan asegurar el ejercicio de los derechos y la toma de decisiones libres e informadas de todas las personas implicadas. Pretendemos abrir el debate y formular propuestas para afrontar el cambio de paradigma que implican dichas nuevas tecnologías de la información ya que, en una sociedad democrática, las medidas de la Administración no deben ser impuestas al ciudadano sin una información previa, veraz y transparente.

Este nuevo Documento ha sido coordinado por las Dras. Llácer, Casado y Buisan, y ha sido elaborado por el *Grupo de Opinión del Observatori de Bioètica i Dret (Grup de Recerca Consolidat Bioética, Dret i Societat)* con la colaboración del *Grup de Recerca en Dret Privat, Consum i Noves Tecnologies de la Universitat de Barcelona (GREDINT)*. Han participado en su preparación todas las personas cuyos nombres y perfiles profesionales se incluyen al final del mismo.

# CONSIDERACIONES GENERALES

## Los retos del big data y la anonimización

La expresión *big data* es un término que designa el tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer correlaciones entre ellos, predecir tendencias y tomar decisiones. Las tecnologías *big data* constituyen un nuevo paradigma e implican cambios organizativos en las empresas y en la propia Administración. Actualmente, las empresas ya no se organizan tanto a través de la mejora de los procesos como en torno a la gestión del dato. Asistimos a una transición hacia la *datificación* y la *monetización* que comporta extraer un nuevo valor de los datos y rentabilizarlos, tanto desde el interés privado como el público, o una combinación de ambos. Es una tendencia inserta en una floreciente industria basada en el conocimiento adquirido a través de la reutilización de los datos y su explotación, que conviene tener en cuenta para contextualizar el debate y entender este cambio de modelo. No obstante, la apuesta por la innovación no puede olvidar los aspectos éticos y los derechos fundamentales de las personas, ni la protección de los ciudadanos en el contexto de estos nuevos avances de las tecnologías. Se trata de examinar esta situación para proponer un nivel de protección firme que suponga en sí mismo una mejora y, por ello, un nivel más avanzado de innovación en este ámbito.

Es crucial señalar que, hasta ahora, la premisa de la *anonimización* del dato ha representado la garantía que permitía cumplir con las regulaciones de protección de datos personales existentes. Se ha venido entendiendo que un conjunto de datos personales, al ser anonimizados, dejan de contener datos de carácter personal, perdiendo así el amparo de la normativa de protección de datos personales, que se pretende rigurosa tanto en la UE como en España pero que, con el avance de las tecnologías informáticas, tras casi veinte años ha devenido en buena medida obsoleta. El problema radica en que, actualmente, está acreditado que la anonimización no garantiza la privacidad de los datos personales, puesto que mediante técnicas de ingeniería informática es posible volver a conectar los datos con la persona a quien pertenecen[9]. La des-

[9] Art. 29 Working Party Opinion 06/2013 on open data and public sector information ('PSI') reuse (1021/00/EN WP207); Art.29 Working Party Opinion 05/2014, on Anonymisation Techniques (0829/14/EN WP216). Véase: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

NARAYANAN, Arvin; FELTEN, Edward W. "No silver bullet: De-identification still doesn't work", 2014. Véase: http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf

NARAYANAN, Arvin; SHMATIKOV, Vitaly. "Robust de-anonymization of large sparse datasets". *Security and Privacy*. IEEE Symposium on IEEE, 2008, pp. 111-125.

DE MONTJOYE, Yves-Alexandre, *et al.* "Unique in the Crowd: The privacy bounds of human mobility". *Scientific*

anonimización y la re-identificación subsiguiente, resultan posibles cuando se dispone de la competencia técnica y los medios necesarios; así, el debate se apoya en un campo más técnico, del que se obtienen informaciones y argumentos que afectan directamente a la base sobre la que se apoya la industria de la venta de datos. Baste saber que la re-identificación puede hacerse por los valores particulares que pueden tomar ciertos datos, hasta ahora considerados como no personales; por ejemplo, se ha demostrado que con un código postal, la fecha de nacimiento y el sexo, es posible re-identificar a la gran mayoría de personas de un *dataset*. De la misma manera que nuestras huellas dactilares nos identifican unívocamente, también ocurre lo mismo con ciertas tipologías de datos. La polémica que subyace es profunda: ¿qué es un dato personal y cómo podemos garantizar su protección?[10], ¿cómo podemos evitar que un conjunto de datos no personales permitan identificar a una persona?

Insistimos en este punto ya que el negocio de la "puesta en valor" depende precisamente de este concepto, ya que la anonimización sería la clave que descartaría la vulneración de las normas de protección de datos personales. Existe un debate abierto sobre la anonimización que, pese a remontarse ya algunos años, podría decirse que no ha hecho más que empezar y está todavía lejos de su fase de resolución. Es una discusión que, a nuestro juicio, resulta crucial para la sociedad del siglo XXI y que aún no ha alcanzado la suficiente presencia en los diversos foros concernidos (legales, éticos, técnicos, empresariales, gubernamentales) y en los que se debería generar el diálogo adecuado para ser, en primer lugar, comprendida, y, en segundo lugar, resuelta o al menos gestionada.

Como se ha dicho, en estos momentos, las evidencias técnicas ya nos muestran que es posible re-identificar a personas concretas a partir de los datos de un conjunto de datos (*dataset*) sobre el cual se han aplicado técnicas de anonimización (o de-identificación). Una persona, o una empresa, puede conseguir la re-identificación si tiene la voluntad (por razones económicas, empresariales, delictivas…), los conocimientos y los medios técnicos para ello (por ejemplo, con los datos sanitarios de un hospital –sin datos personales– y acceso a los datos personales de otro *dataset* –digamos, un censo–). Parece evidente que, en el caso de los datos de salud, es fácil encontrar ese hipotético "*adversario*" con la motivación y los recursos para poder hacerlo y, por lo tanto, es acertado cuestionar la validez de las iniciativas de intercambio de datos sensibles que estén basadas en técnicas de anonimización. En el ámbito jurídico, el incierto recurso a la "anonimización", entendida como una solución definitiva pero irremediablemente en crisis, viene propiciado por la actual normativa de protección de datos cuyo origen se halla en una Directiva

*reports*, 2013, vol. 3.

OHM, Paul: "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". *UCLA L. Rev*. 2009-2010, p. 731.

[10] Paul M. Schwartz & Daniel Solove: "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *86 N.Y.U. L. Rev*. 1814 2011.

europea del año 1995, muy anterior al fenómeno del *big data*, y subyace en la Ley estatal 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Sin embargo, desde el momento en que el propio anonimato deviene incierto es perentorio encontrar una base que legitime el análisis de datos personales de salud a gran escala. De no ser así, se abre la puerta a usos no deseados de esos datos ya que su titular, habiendo dado su consentimiento para determinadas acciones en el ámbito sanitario y de investigación, en realidad pierde el control y queda desprotegido pues –con una falsa concepción de la protección de datos y del secreto profesional– desconoce que sus datos pueden haber sido utilizados o cedidos para otros fines, ni deseados ni efectivamente consentidos.

Este Documento no pretende rechazar, sin más, este nuevo modelo de negocio que centra la atención del mercado y en el que ya estamos inmersos, sino que aspira a alertar sobre sus riesgos a los ciudadanos y a los poderes públicos que regulan y controlan la actividad en el ámbito sanitario y de investigación. Entre nosotros no se ha consolidado la conciencia social de la importancia de proteger los datos y su relación con el derecho fundamental a la intimidad y a la no discriminación. Carecemos de una cultura de la privacidad en materia de datos personales que nos permita comprender cómo puede afectarnos el hecho de que una empresa acumule y rentabilice nuestra información y tenga en sus manos un instrumento de poder para tomar decisiones que pueden afectarnos[11]. Por ejemplo, el análisis masivo de datos puede utilizarse para descubrir efectos secundarios de medicamentos, pero también permite crear perfiles de riesgo –incluso desconocidos por los afectados– que podrían utilizarse para "justificar" la denegación de una póliza de seguro.

Es evidente la urgencia de un debate que señale la vulnerabilidad de las personas ante los riesgos de discriminación basados en perfiles y patrones de comportamiento creados con fines que el afectado no puede controlar, y sobre la adaptación de las normas a los retos éticos y sociales planteados por las posibilidades que proporciona el despliegue de las tecnologías *big data*. Justamente es este el núcleo del conflicto que hay que abrir al debate público con la implicación de la ciudadanía, creando una cultura de privacidad acorde con los nuevos tiempos y las nuevas realidades.

## Sobre el proyecto VISC +

Un ejemplo de reutilización de datos que a nuestro entender resulta cuestionable es el proyecto VISC+, impulsado por la Agència de Qualitat i Avaluació Sanitària de Catalunya (AQuAS) de la Generalitat de Catalunya, que tiene como objetivo –según describen sus promotores– poner la

[11] Cohen, Julie: "What Privacy is for" 126 *Harv. L. Rev*. 1904 2012-2013.

información sanitaria a la disposición de los ciudadanos, las empresas y la investigación, para mejorar los servicios de salud y la investigación y para 'poner en valor' el conocimiento.

El mencionado proyecto se nutre de las distintas bases de datos sanitarios existentes en el sistema, entre otros el SIDIAP (Sistema de información para el desarrollo de la investigación en la atención primaria) y, especialmente, de la HC3 (Historia clínica compartida de Cataluña) que recoge los datos asistenciales y de consumo farmacéutico, junto con otras informaciones relevantes referentes a la identificación y situación socio-sanitaria de cada ciudadano atendido en el sistema público; la HC3 contiene, también, la información de las pruebas analíticas y diagnósticas que incluyen datos metabólicos y bioquímicos, así como datos de diagnóstico genético que identifican a portadores de enfermedades genéticas hereditarias, o determinan riesgo o susceptibilidad de padecer enfermedades más complejas. Estas bases de datos conllevan la existencia de "ficheros de usuarios", de los cuales es responsable el Departament de Salut de la Generalitat de Catalunya. Si bien los macro ficheros de datos están protegidos por la normativa ya existente –en especial por la Ley Orgánica de Protección de Datos (LOPD) y el Reglamento que la desarrolla–, esta regulación resulta insuficiente ya que su aplicación ha sido superada por la nueva tecnología *big data* –como se ha indicado– y no evita los usos indebidos y discriminatorios[12].

La HC3 tiene los objetivos explícitos de: a) mejorar la atención de la salud de los ciudadanos mediante una herramienta que facilite el trabajo de los profesionales sanitarios; b) propiciar un nuevo modelo asistencial al permitir a los centros sanitarios de la red de asistencia pública el acceso y la consulta de forma inmediata, segura y confidencial de la información relevante disponible sobre los pacientes. Como es evidente, los datos que contiene son sensibles en extremo, y su recogida y tratamiento se justifican en la eficacia a la hora de prestar una buena asistencia, no solo en el centro habitual sino en toda la red pública catalana[13] ya que la HC3 permite el acceso de manera organizada, y bajo parámetros de seguridad y confidencialidad, a las historias clínicas de los centros sanitarios de la red asistencial. Esta herramienta debe ofrecer beneficios tanto a los profesionales sanitarios como a la ciudadanía y al propio sistema de salud. Por ello, el ciudadano tiene derecho a conocer quién dispone de sus datos personales y con qué finalidad; y también a exigir responsabilidades si considera que se está haciendo de los mismos un uso indebido o distinto de aquellos para los que hubiera otorgado el consentimiento en su momento. Cuando la HC3 se implantó, ni se informó suficientemente a los ciudadanos de dicha

---

[12] Como el Grupo de Opinión ya advirtió en el *Documento sobre pruebas genéticas de filiación*, Barcelona: Signo, 2006. Disponible en formato PDF en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/07899.pdf

[13] Existe un proyecto, de mayor alcance territorial, desarrollado en 12 países de la UE, en el marco de www.epSOS.eu, del que forman parte: Alemania, Austria, R. Checa, Dinamarca, Eslovaquia, España, Francia, Grecia, Holanda, Italia, Reino Unido y Suiza. En España participan tres CCAA: Andalucía, Castilla la Mancha y Cataluña dentro del PLAN AVANZA para la modernización de los servicios de las administraciones públicas.

recogida masiva de datos, ni se indicó en ningún momento que pudieran llegar a reutilizarse para otras finalidades, incluso comerciales. Tampoco cabría considerar que la cesión de los datos de los usuarios del sistema público para finalidades no asistenciales fuera el "precio" de la asistencia gratuita, pues es improcedente exigir una contraprestación, ya que esta conllevaría que tal asistencia dejara de ser gratuita.

La HC3, pese a ser recogida y estructurada por los profesionales asistenciales, pertenece al paciente y, por esta razón, las entidades asistenciales reciben peticiones relacionadas con el ejercicio de los derechos que la normativa vigente en protección de datos reconoce a los ciudadanos: derechos de acceso, rectificación, cancelación y oposición (los llamados derechos ARCO). La finalidad de este conjunto de derechos es impedir un tratamiento de los datos personales ilícito y lesivo para la dignidad y el derecho del afectado *(habeas data)*, así como garantizar el ejercicio del más general derecho a la intimidad. Así, los usos de los datos recogidos en la HC3 deben limitarse a la asistencia (junto con los fines científicos –epidemiológicos, investigación y docencia– o encaminados a la mejora de los servicios públicos, que la normativa actual ya autoriza) y es absolutamente preciso establecer garantías que eviten el tráfico de datos y cualquier uso indebido de las empresas del ámbito de la salud (seguros médicos, corporaciones farmacéuticas, entidades financieras y otros). Por ello, el Proyecto VISC +, tal como en estos momentos está previsto que se lleve a cabo, genera dudas importantes, tanto de carácter bioético como estrictamente jurídicos, que conviene debatir para prevenir su potencial uso discriminatorio.

## Problemas relevantes del proyecto VISC+

### 1.- Denominación equívoca del Proyecto

Consideramos que la propia denominación del proyecto es equívoca y no se adecua al "principio general de lealtad en la recogida y tratamiento de datos", porque induce a pensar que el único resultado del proyecto consiste en mejorar las condiciones de vida y la salud. Cualquier usuario a quien se pida el consentimiento para que sus datos personales de salud sean tratados en el marco de un proyecto así llamado[14] puede pensar, erróneamente, que colabora en un programa que solo le reportará beneficios. Esto puede relacionarse con una práctica contraria al principio jurídico de buena fe, más aun cuando los datos se recaban en un momento especialmente sensible, que puede distorsionar la capacidad de escoger con pleno conocimiento de causa, induciendo a facilitar información que de otro modo no se habría proporcionado. La lealtad es un valor fundamental en el marco de la LOPD, que prohíbe expresamente la recogida y el tratamiento de datos por medios fraudulentos o desleales, y afecta de manera directa al principio de calidad de los datos.

[14] VISC+ significa en catalán "VIVO más".

## 2.- Limitación de las finalidades en el tratamiento de los datos

Como bien se recoge en el informe elaborado por el *Grupo Europeo de Ética de las ciencias y de las nuevas tecnologías* (GEE), de la Comisión Europea, en la recogida y tratamiento de datos de carácter personal las entidades públicas y las privadas deben fundamentar su actividad en el principio de "limitación de la finalidad"[15]; es decir, que este tipo de datos no deben ser recogidos ni tratados para cualquier uso, sino sólo con objetivos específicos y legítimos que se hayan prefijado. Además, los datos no han de estar a disposición de "quien los quiera utilizar" y los ciudadanos deben disponer de mecanismos efectivos para controlar y modificar las informaciones que les conciernen. Insiste también dicho informe en que cualquier posible cesión de datos con fines comerciales sólo debe hacerse con el consentimiento expreso de las personas afectadas, y con conocimiento del tipo de datos que se tratarán, con qué objetivo, durante cuánto tiempo y, si se van a relacionar o cruzar con otros datos procedentes de diferentes fuentes.

Resulta de especial importancia, en el marco del proyecto que aquí se analiza, conseguir una protección gradual de los datos en función de la finalidad del uso, distinguiendo cuidadosamente las finalidades sanitaria, epidemiológica y de investigación y docencia de las finalidades empresariales privadas basadas en la investigación, a las que hay que exigir el nivel de protección más elevado. Ahora bien, el proyecto VISC+ equipara tratamientos que tienen fines totalmente diferentes y esta confusión afecta a la legitimación para tratar los datos sanitarios, personales, que son datos especialmente sensibles y que, en consecuencia, están sometidos a una protección especial.

Como se ha indicado, la ley ampara el uso de datos del paciente para llevar a cabo la asistencia sanitaria y para la investigación y mejora de los servicios públicos. Si se quiere ir más allá y facilitar su utilización con fines no previstos ni autorizados –entre los cuales los intereses comerciales de empresas privadas cuyo producto depende de la investigación, entre otros factores– es necesario un debate social previo sobre la concurrencia de los intereses públicos y privados en la investigación, con el objeto de definir sus contornos éticos y el nivel de protección que se va a reconocer al ciudadano cuando empresas con intereses privados traten datos de salud. El *empoderamiento* del ciudadano se construye con información completa, clara y veraz sobre el uso de sus datos y reconociendo su facultad de controlar el tratamiento, consintiéndolo u oponiéndose al mismo.

---

[15] EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES: Ethics of Security and Surveillance Technologies. Opinión n. 28, 20 de mayo de 2014. Véase: http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_ security_surveillance_technologies.pdf

## 3.- Habilitación legal *vs.* consentimiento

El contar con la necesaria legitimación es el requisito básico para permitir el acceso de terceros a informaciones o datos que pertenecen al ámbito personal de los afectados. Se debe distinguir entre la legitimación legal, y la voluntaria, basada esta segunda en el consentimiento libremente otorgado. La primera permite tratar los datos con finalidades relacionadas con la atención sanitaria, la calidad y gestión del servicio o fines científicos (epidemiológicos, investigación y docencia). Esta legitimación procedente de una ley se justifica en el interés público, respetando siempre escrupulosamente la confidencialidad de los datos recogidos y obligando a motivar la solicitud de uso de los mismos. Consideramos que el proyecto VISC+, habiendo sido aprobado por un mero "Acuerdo de gobierno", no cuenta con habilitación legal suficiente para la reutilización de datos sanitarios, ya que las leyes de sanidad sólo legitiman para tratar los datos de los pacientes con fines directamente asistenciales, investigadores u organizativos. El segundo tipo de legitimación, la voluntaria, proviene siempre del consentimiento expreso del paciente y es la que se precisa para tratar datos con fines estrictamente privados, es decir, sin interés público evidente; este consentimiento es el que se requiere para utilizar los datos de los usuarios en el desarrollo de las industrias sanitarias, farmacéuticas y de biotecnología, o la promoción y comercialización de sus productos. Consideración especial merecen los datos genéticos por la complejidad que supone su titularidad compartida por un núcleo familiar.

Partiendo de la existencia del "*partenariado* público-privado" en el sistema sanitario e investigador, el problema se centra en cómo se articula la legitimación para usar la información de salud y reutilizarla. A nuestro juicio, debe plasmarse en una ley y es preciso tener en cuenta la gran asimetría –de información e incluso de poder– existente entre el ciudadano, que sufre una enfermedad y necesita curarse, y el profesional que le va a pedir el consentimiento, tanto para procurarle la asistencia médica más adecuada como para el tratamiento de los datos personales de salud. Hay que tener claro que se trata de consentimientos diferentes, y que el acceso a la prestación sanitaria pública no se puede condicionar al consentimiento para tratar datos con otros fines, ni justifica la solicitud de datos adicionales. La conclusión es que la obtención del consentimiento debe someterse a garantías, a fin de compensar la situación de desequilibrio en que se encuentra el usuario de los servicios sanitarios públicos en momentos en los que puede estar especialmente preocupado por su salud –lo que genera una situación de vulnerabilidad– y que piensa a priori que todos los datos que se le piden se encaminan a su tratamiento y son necesarios para prestarle la asistencia que necesita y que constituye la razón por la que ha acudido al sistema sanitario.

## 4.- Valor y riesgo

En este contexto, el proyecto VISC+ se presenta con el objetivo de "poner en valor" la enorme cantidad de datos de los que dispone el Departamento de Salud y con el fin de "reutilizar" estos datos para finalidades inicialmente no previstas y que, por ello mismo, el usuario no conoce. La

expresión "poner en valor" mencionada tiene interpretaciones diferentes: por un lado, se trataría de poner a disposición de centros de investigación, centros de estudios epidemiológicos y de salud pública, y centros de docencia que así lo soliciten, datos de salud de los ciudadanos con el objetivo de contribuir al progreso del conocimiento en los ámbitos específicos mencionados y también, en último término, a la mejora de la atención sanitaria y la prevención, cosas perfectamente legítimas y deseables y que, reiteramos, la legislación ya permite. Pero, por otro lado, incluye una interpretación mucho más laxa, que implicaría poner estos *big data* sanitarios a disposición de empresas que difícilmente entrarían en los ámbitos que se acaban de mencionar. Si tenemos en cuenta el principio bien conocido según el cual "*big data is big business",* el escenario más probable sería el de una pura y simple venta de los datos de salud de los ciudadanos en beneficio de la empresa que esté interesada en hacer rentable esta información y que disponga de los medios para hacerlo. Hay que tener siempre en cuenta que la tecnología no es el problema, sino la dirección que le imprime quien la usa y la financia. Así, el marco que plantea el Visc+ permitiría a las empresas implicadas extraer un valor meramente comercial de los datos.

Los riesgos potenciales a que se refiere este Documento, no son hipotéticos, ni remotos: es suficiente con analizar la posibilidad de construir perfiles de conducta sobre datos anónimos, que se pueden utilizar en cualquier momento para tomar decisiones automatizadas sobre las personas. Basta un paseo por internet para encontrar una buena cantidad de empresas dedicadas a la compraventa de datos y cómo las que los poseen –originados en la prestación de otros servicios–, crean a su vez otras nuevas empresas y líneas de negocio dedicadas a la reutilización de estos datos consiguiendo perfiles muy precisos mediante sucesivos cruces de información y demás procesos de "enriquecimiento del dato".

## 5.- Control de los datos

Precisamente en razón de evitar la pérdida de control de los datos y los posibles abusos, tiene sentido establecer funciones de *Data Governance* (es decir, el control del tratamiento y la gestión de los datos) que deben corresponder a las entidades públicas, garantes del escrupuloso respeto de los derechos fundamentales de los ciudadanos, con independencia de cómo se suministren los servicios profesionales por parte de las empresas adjudicatarias. Estas funciones de *gobernanza* deben incluir aspectos como: la seguridad y calidad de los datos, la privacidad, los procesos de anonimización, la trazabilidad, las políticas de permanencia de los datos, el enriquecimiento de datos (poniendo limitaciones a las fuentes o bases de datos con los que se pueden relacionar o cruzar). La preferencia por las garantías que otorga lo público deriva de las específicas obligaciones de transparencia y rendición de cuentas que la Administración tiene, si bien la responsabilidad compartida exigiría también transparencia y rendición de cuentas al sector privado. La Declaración Universal de Bioética y Derechos Humanos de la UNESCO, establece –en su artículo 14– el novedoso principio de responsabilidad social en salud que resulta del todo

pertinente en este contexto y atañe también a la especial atención que se requiere para evitar los conflictos de interés en este delicado campo.

El proyecto VISC+ habla de gobernanza, pero meramente de carácter interno mientras que en el presente Documento se propone un control externo y representativo de la sociedad. El mismo Informe de la Autoridad Catalana del Protección de Datos (APDCAT) ya señala que el VISC+ merece un régimen específico de seguridad aún más estricto. Según este informe, el Departament de Salut es "responsable" del tratamiento de los datos, a efectos legales. En cambio "la entitat" (AQuAS) es "encargada" de su tratamiento. Asimismo, la mecánica prevista en el proyecto VISC+ para la explotación de datos también es motivo de preocupación ya que la empresa adjudicataria recibiría los datos supuestamente anonimizados a cambio de un precio o tasa; hay que advertir que en el mencionada proyecto también se dice que el adjudicatario participaría en el proceso de verificación de la anonimización y en la materialización de un "código anónimo de la persona" antes de transferir los datos a los usuarios finales. Se desconoce si sería esta misma empresa adjudicataria quien se responsabilizaría de "definir, construir y poner en marcha un catálogo de servicios útil, eficiente, competitivo e innovador, de contrastar las necesidades del mercado y los clientes finales, y de definir un plan de difusión y de comercialización, canalizando de manera adecuada la demanda del mercado nacional e internacional".

Consideramos que, en el modelo VISC+ no queda en absoluto claro si serían las empresas adjudicatarias quienes decidirían a quién traspasan los datos de salud, presuntamente a cambio de compensaciones económicas. Contrapartidas que tampoco se precisan y de las que ni se menciona cómo revertirían en los ciudadanos. Por ejemplo, ¿se cedería la base de datos de enfermos de hepatitis C para desarrollar fármacos que después se pretenderían vender a 70.000€ cada tratamiento? Justamente esta cuestión sería la clave que condicionaría hasta qué punto los clientes o usuarios finales del proyecto estarían dispuestos a contribuir.

## 6.- Evaluación del impacto

El proyecto VISC+ no incluye ninguna evaluación del impacto que su puesta en marcha pueda tener sobre el derecho a la intimidad de los usuarios, como sería pertinente teniendo en cuenta que estamos hablando de datos tan sensibles como los de salud, en la línea de lo que propone el proyecto de Reglamento europeo de protección de datos. La valoración del impacto –también ético y social– sería, obviamente, un requisito de cualquier ley que amparara el proyecto VISC+. Tampoco el Proyecto especifica en ninguna parte si los usuarios tienen que dar previamente su consentimiento para el trasvase de datos que implica, ni si entiende que este consentimiento no sería necesario dada la interpretación laxa del concepto de investigación a que se ha hecho referencia más arriba y que no diferencia entre el interés público y el interés privado. El proyecto VISC+ no incluye ninguna evaluación del impacto que su puesta en marcha pueda tener sobre el derecho a la intimidad de los usuarios, como sería pertinente teniendo en cuenta la sensibilidad de

los datos de salud, en la línea de lo que propone el proyecto de Reglamento europeo de protección de datos.

Además, finalmente pero no menos importante, en ningún momento se explica claramente en el VISC+ cómo el beneficio económico que se obtuviera del Proyecto repercutiría favorablemente en los ciudadanos y en el sistema sanitario público. Parece evidente que, siendo los datos tan valiosos, cuando hay beneficios y negocio, los ciudadanos deberían contar con contrapartidas bien establecidas. Consideramos que el lucro es un fin lícito, pero no el bien primordial al que todos los demás valores y derechos deban subordinarse. El Convenio de Derechos Humanos y Biomedicina del Consejo de Europa, en vigor en nuestro país desde el 2000, establece –en su artículo 2– que los intereses de la ciencia o de la sociedad no deben prevalecer nunca sobre los del individuo; sobre esta premisa pivota todo el sistema de ciencia y tecnología y, en especial, el sistema sanitario y de investigación.

## 7.- La experiencia National Health Service

Es importante remarcar que las experiencias en la línea del Proyecto VISC + que se han llevado a cabo en países de nuestro entorno han generado conflictos muy significativos que llevan a extremar las medidas de prudencia antes de emprender proyectos de este tipo. En efecto, la supuesta anonimización de datos de salud y atención sanitaria recogidos por el *NHS Information Centre* (NHS-IC), entre 2005 y 2013, no ha impedido que diferentes empresas hayan re-identificado a las personas a quienes hacían referencia estos datos, generando perjuicios diversos; por ejemplo en el precio de las primas de riesgo de los seguros. La consecuencia ha sido una moratoria con el fin de reorganizar el procedimiento de cesión de los datos de manera que sea más transparente y garantice de forma más eficaz los derechos a la intimidad y a la confidencialidad. Actualmente el procedimiento de tratamiento y cesión de los datos está sometido, en todo momento, a auditoría y control público. Para ello se ha creado el *Care Data AdvisoryGroup,* grupo consultor cuya misión es fortalecer la protección de los derechos de los ciudadanos en el ámbito sanitario, y la *National Data Guardian,* a fin de velar por la seguridad de los datos de salud.

## RECOMENDACIONES

1. *Generar y potenciar una cultura ciudadana de la privacidad en materia de datos personales.* Acumular información sobre una persona representa adquirir un poder de decisión sobre ésta; por lo tanto, los medios para controlar quién trata nuestros datos, cómo los capta y con qué fin los usa se convierten en instrumentos de libertad personal y colectiva.
2. *Informar y formar sobre el alcance real de que los procesos de anonimización de los datos ya no garantizan la irreversibilidad.* Es factible actualmente la des-anonimización, re-identificación, o revelación de datos personales de conjuntos de usuarios y de usuarios individuales, pues las herramientas informáticas empleadas pueden servir tanto para esa finalidad como para la contraria.
3. *Alertar sobre la necesidad de redefinir el concepto mismo de "datos personales" sobre el que se asienta la legislación actual:* Es importante remarcar que el problema no es únicamente la transformación de los datos considerados personales en un conjunto de datos, pues incluso eliminando estos datos personales es posible llegar a re-identificar a una persona concreta.
4. *Aplicar escrupulosamente el principio que requiere que los datos recabados sean adecuados a la finalidad que motiva su recogida, y exigir que se solicite y se obtenga el consentimiento expreso de los usuarios para la utilización de los datos de salud con fines diferentes a aquellos para los que se obtuvieron, implementando mecanismos eficaces para otorgar, o denegar, dicho consentimiento*. En el caso de datos genéticos, el consentimiento debe ser especialmente riguroso dada la posible afectación a otros miembros del núcleo familiar.
5. *Potenciar el proceso de información y de debate –basado en una honesta ponderación de riesgos y beneficios, ventajas y perjuicios– ante la puesta en marcha de un proyecto como el VISC +,* encaminado a la explotación de datos de salud que pertenecen a los ciudadanos, aunque estén en poder de la Administración, a fin de que puedan pronunciarse sobre la conveniencia de llevar a la práctica tal proyecto.
6. *Establecer mecanismos de control en el tratamiento de datos y concretar las funciones de "Data Governance" que son responsabilidad de los organismos públicos.* Los procesos de anonimización del dato deben llevarse a cabo dentro del perímetro interno de la Administración por las garantías que otorgan las obligaciones de transparencia y rendición de cuentas que dicha Administración tiene, si bien la responsabilidad compartida exige también transparencia y rendición de cuentas al sector privado, especialmente en las redes mixtas público-privadas.
7. *Controlar de forma específica y reforzada la seguridad en el tratamiento de los datos sanitarios para garantizar en todo momento su correcto uso y evitar la comercialización, que no cuente con consentimiento expreso y no prevea de forma clara la manera en que el beneficio revierta a los ciudadanos.*

Para ello debe crearse un órgano de gobernanza externo representativo de la sociedad catalana e independiente de los agentes implicados. Sus funciones consistirían en supervisar la gestión de los ficheros en todas las etapas, verificar la trazabilidad, detectar conflictos de interés y malas prácticas, así como identificar posibles infracciones y responsabilidades e informar públicamente de su actuación y resultados. De esta manera, el ciudadano podría dirigirse a él para saber quién dispone de sus datos personales y con qué finalidad.

Para llevar a cabo sus funciones dicho organismo debería promover y aplicar un *Código Ético para la Reutilización de Datos de Salud*.

8. *Reforzar la formación en deontología y ética profesional de los implicados en la custodia de los datos*, señalando que toda persona que tenga acceso o trate datos tiene el mismo deber de proteger y promover los derechos y libertades fundamentales de los implicados. El derecho a la intimidad, la confidencialidad y la no discriminación, son pilares del sistema de salud y de investigación.
9. *Recordar que los comités de ética deben contribuir al desarrollo de la cultura de respeto por la intimidad y la confidencialidad de los datos personales ya que, en su ámbito de actuación, son los primeros garantes de estos derechos*. Los miembros de los comités de ética, para poder colaborar en la toma de decisiones ponderadas y proporcionales, deben formarse en los aspectos éticos, técnicos, jurídicos y sociales de las tecnologías y la especial protección que requieren los datos sanitarios, así como prestar atención a no actuar de forma que les convierta en meros mecanismos de cobertura de intereses ajenos.

# NORMATIVA DE REFERENCIA

## Internacional

- Consejo de Europa: Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997.
- UNESCO: Declaración universal sobre Bioética y Derechos Humanos, de 19 de octubre de 2005.

## Europea

- Carta de los Derechos Fundamentales de la Unión Europea (DOUE núm. 83, de 30 de marzo de 2010).
- Directiva 1995/46/CE, de 24 de octubre, del Parlamento y del Consejo, sobre Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

## España

### Sistema sanitario

- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.
- Ley 33/2011, de 4 de octubre, General de Salud Pública.

- Llei 21/2000 (del Parlament de Catalunya), de 29 de desembre, sobre els drets d' informació concernent la salut i l'autonomia del pacient, i la documentació clínica.
- Llei 16/2010 (del Parlament de Catalunya), de 3 de juny, de modificació de la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

### Sistema de investigación

- Real Decreto 223/2004, de 6 de febrero, por el que se regulan los ensayos clínicos con medicamentos.
- Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.
- Ley 14/2007, de 3 de julio, de Investigación biomédica.
- Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

### Protección de datos de carácter personal

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

### Reutilización de la información del sector público

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, sobre reutilización de la información del sector público.

# MEMBRES DEL GRUP D'OPINIÓ DE L'OBSERVATORI DE BIOÈTICA I DRET QUE HAN ELABORAT AQUEST DOCUMENT

*Maria Rosa Llàcer*
Catedràtica de Dret Civil, Universitat de Barcelona. Directora del Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT).

*María Casado*
Catedràtica d'Universitat. Directora de l'Observatori de Bioètica i Dret, del Màster en Bioètica i Dret de la Universitat de Barcelona i del GRC Bioètica Dret i Societat. Titular de la Càtedra UNESCO de Bioètica de la Universitat de Barcelona. Membre de la Comissió de Bioètica, Universitat de Barcelona.

*Lídia Buisan*
Metgessa i advocada. Professora d'Ètica Mèdica, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Pilar Antón*
Professora Titular de Legislació i Ètica Professional de l'Escola Universitària d'Infermeria, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret i de la Comissió de Bioètica, Universitat de Barcelona.

*Àngels Avecilla*
Ginecòloga. Cap de secció de Salut Sexual i Reproductiva, Badalona Serveis Assistencials. Màster en Bioètica i Dret, Universitat de Barcelona. Membre del Comitè d'Ètica d'Investigació de l'Hospital Germans Trias i Pujol.

*Anna Badia*
Catedràtica de Dret Internacional Públic, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Immaculada Barral*
Professora Titular de Dret Civil, Universitat de Barcelona. Membre del Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT).

*Blanca Bórquez*
Advocada de la Corte Suprema de Chile. Màster en Bioètica i Dret, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Maria Jesús Buxó*
Catedràtica d'Antropologia de la Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret i de la Comissió de Bioètica, Universitat de Barcelona.

*Lluís Cabré*
Metge. Cap de la Unitat de Cures Intensives, Hospital de Barcelona. President de l'Associació de Bioètica i Dret. Membre de l'Observatori de Bioètica i Dret (Universitat de Barcelona) i del Comitè Consultiu de Bioètica de Catalunya.

*Mirentxu Corcoy*
Catedràtica de Dret Penal, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Fernando García López*
Centro Nacional de Epidemiología, Instituto de Salud Carlos III, Madrid. Màster en Bioètica i Dret, Universitat de Barcelona.

*Ricardo García Manrique*
Professor Titular de Filosofia del Dret, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Carmelo Gómez*
Professor Titular de Filosofia del Dret, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Maria Dolors Gramunt*
Professora Titular de Dret Civil, Universitat de Barcelona. Membre del Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT).

*Carlos Humet*
Metge i Director de l'Hospital de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Itziar de Lecuona*
Professora del Departament de Salut Pública, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Gemma Marfany*
Professora Titular de Genètica, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Joaquim Martínez Montauti*
Metge. Coordinador del Servei de Medicina Interna de l'Hospital de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Isabel Miralles*
Professora Titular de Dret Civil, Universitat de Barcelona.

*Esther Mitjans*
Professora Titular de Dret Constitucional, Universitat de Barcelona. Antiga directora de l'Autoritat Catalana de Protecció de Dades (ACPD).

*Mónica Navarro-Michel*
Professora de Dret Civil, Universitat de Barcelona. Vicedegana de la Facultat de Dret. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Ismael Peña-Lopéz*
Professor de Dret i Ciència Política, Universitat Oberta de Catalunya. Membre del Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT).

*Glòria Pérez*
Metgessa especialista en Medicina Preventiva i Salut Pública.

*Francesca Puigpelat*
Catedràtica de Filosofia del Dret, Universitat Autònoma de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Rosa Ros*
Metgessa. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Albert Royes*
Secretari de la Comissió de Bioètica, Universitat de Barcelona. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Gemma Rubio*
Professora de Dret Civil, Universitat de Barcelona. Membre del Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT).

*Ana Sánchez Urrutia*
Consultora de Bioètica del Secretari Nacional de Ciència i Tecnologia de Panamà. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.

*Josep Santaló*
Catedràtic de Biologia Cel·lular, Universitat Autònoma de Barcelona. President de la Comissió d'Ètica en Experimentació Animal i Humana de la UAB. Membre de l'Observatori de Bioètica i Dret, Universitat de Barcelona.